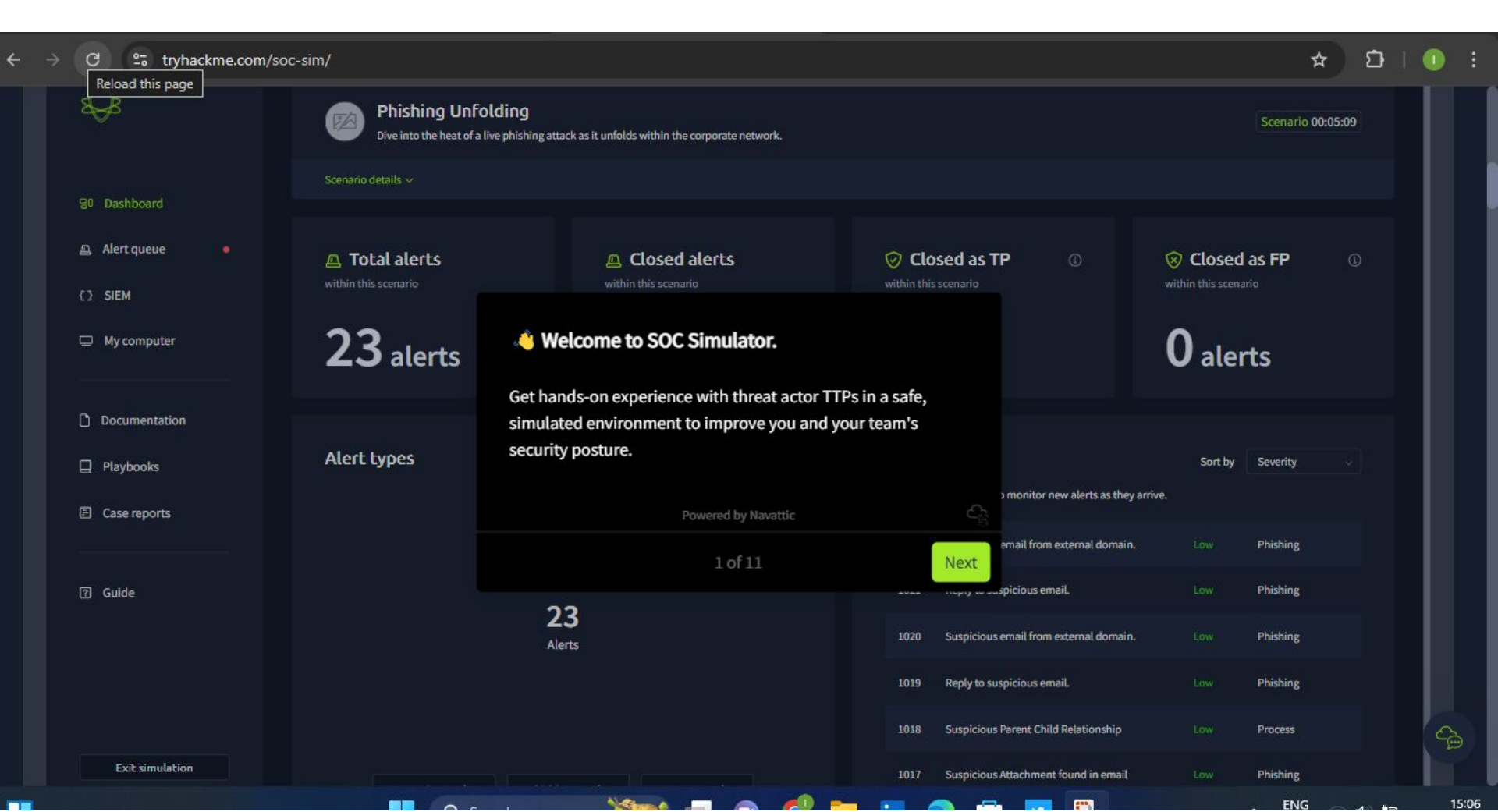
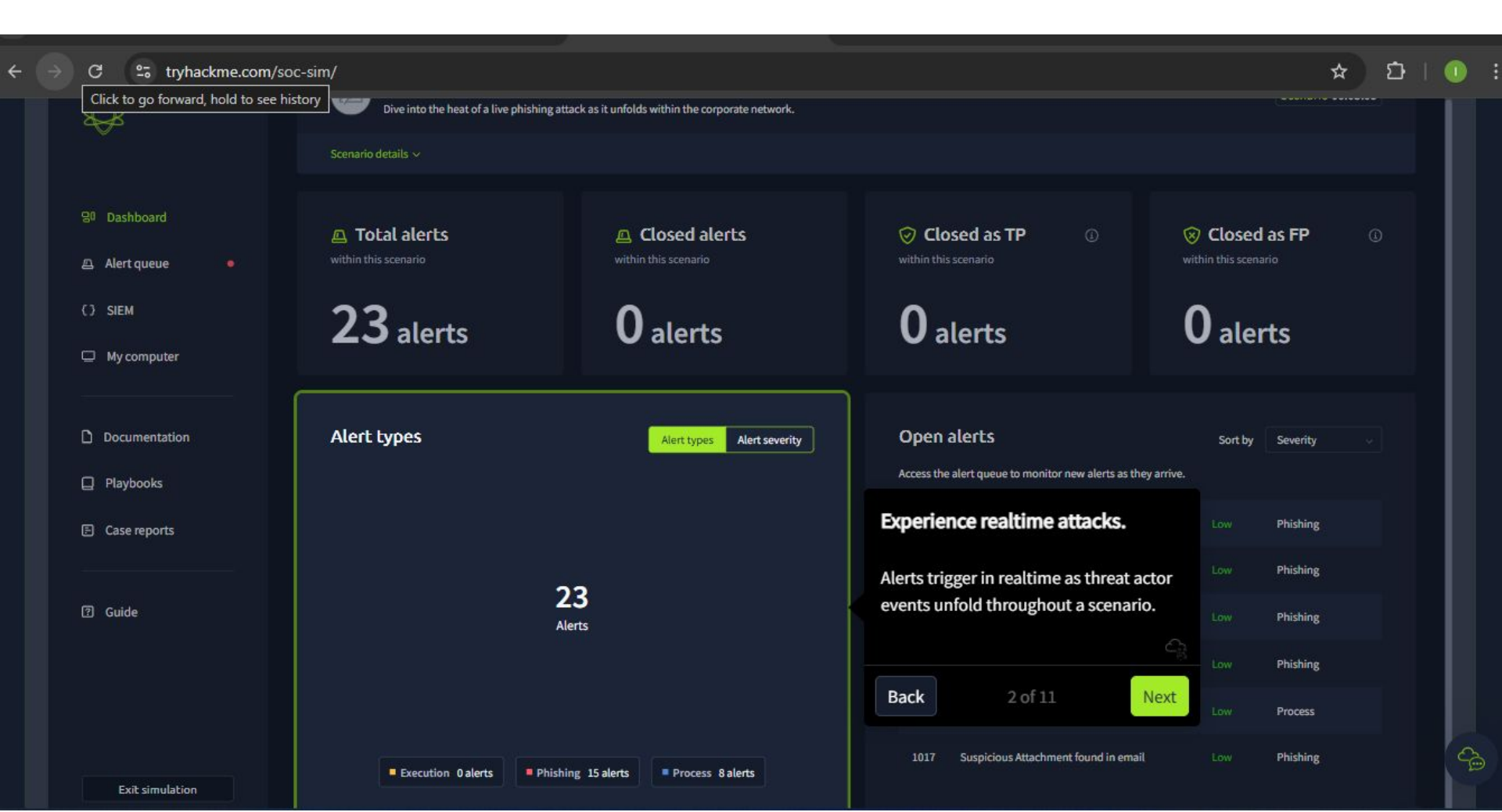
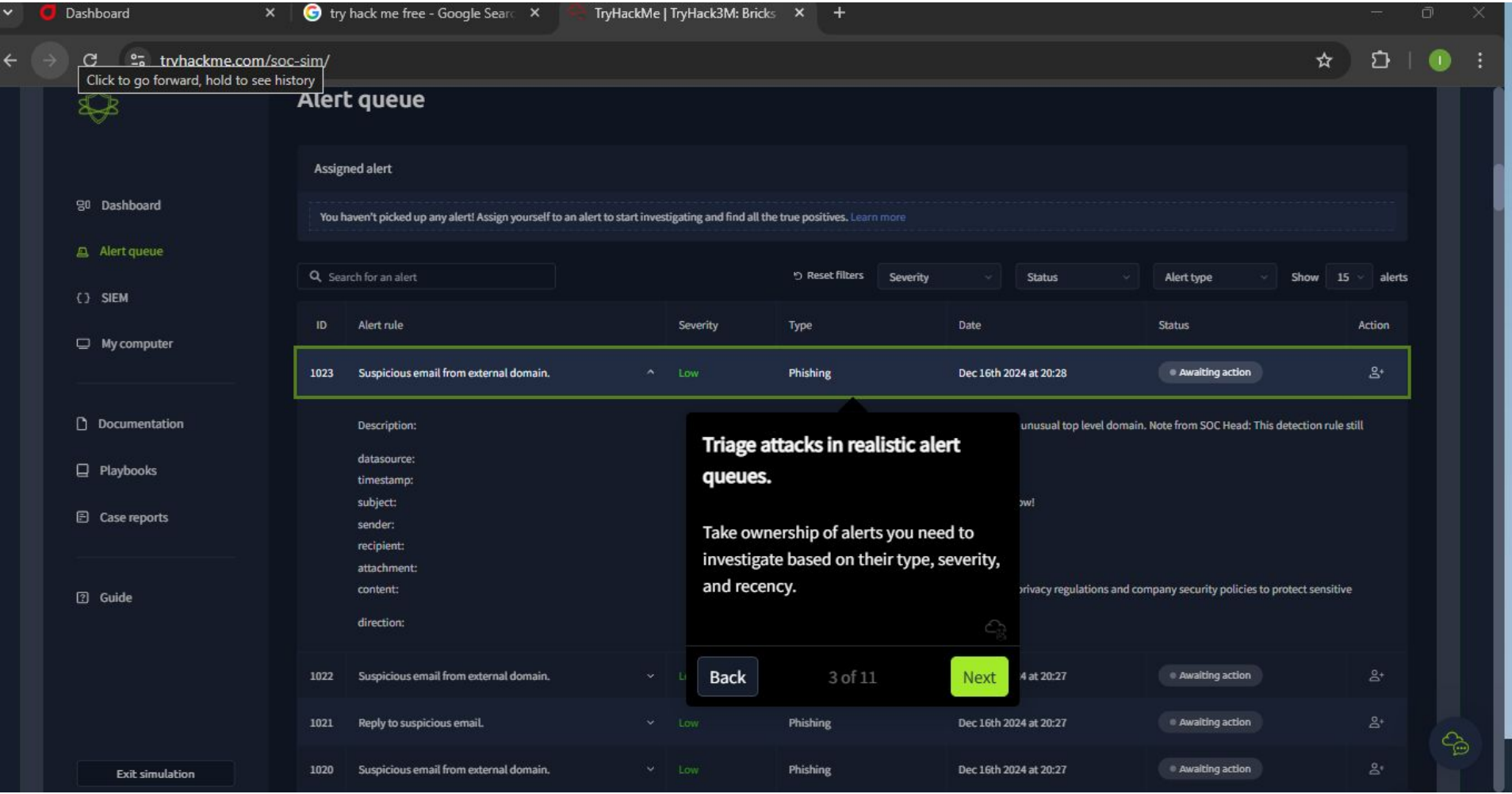
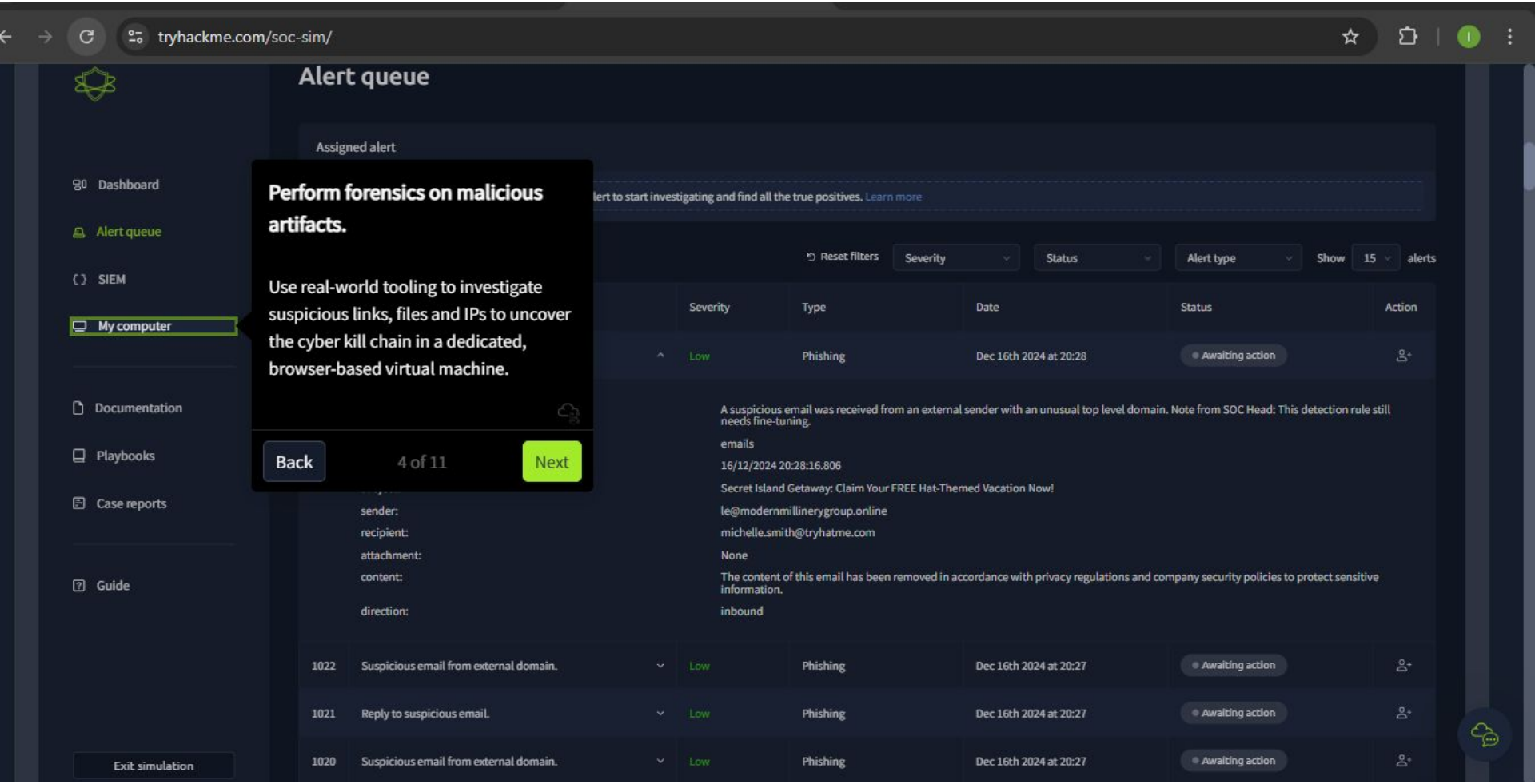
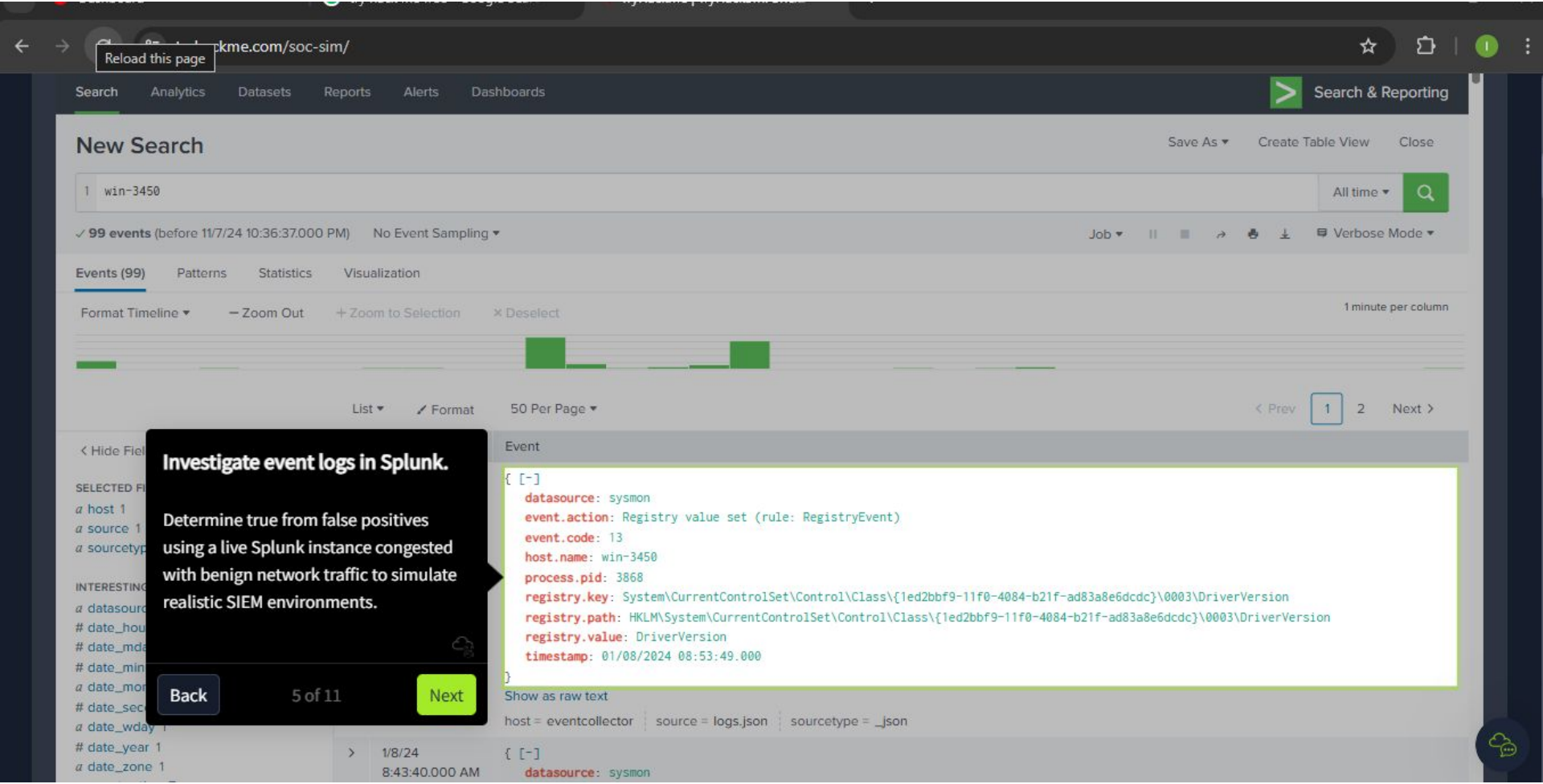
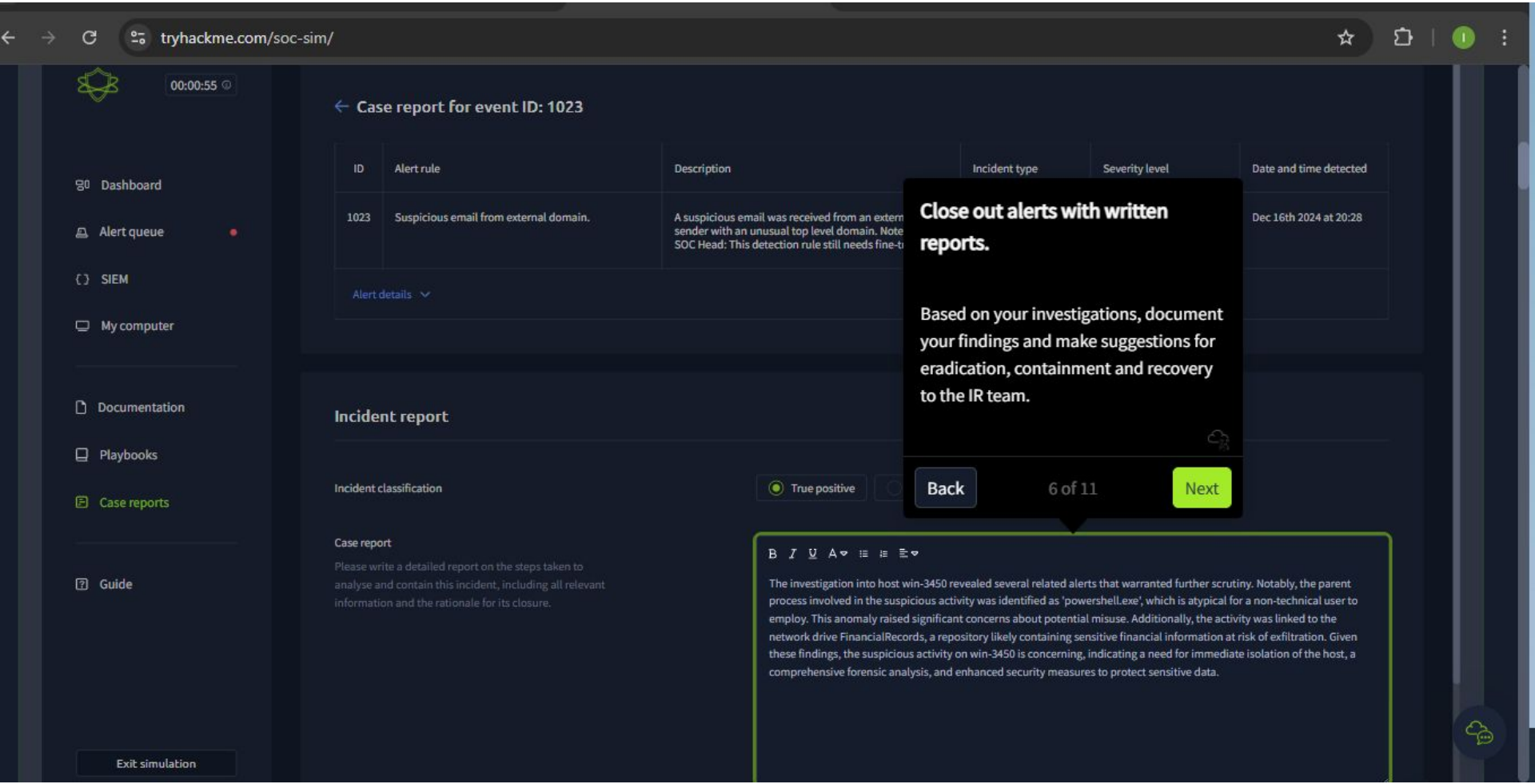

tryhackme.com/soc-sim/
Reload this page
Phishing Unfolding
Dive into the heat of a live phishing attack as it unfolds within the corporate network.
Scenario 00:05:09
Scenario details
Dashboard
Alert queue
SIEM
My computer
Documentation
Playbooks
Case reports
Guide
Exit simulation
Total alerts
within this scenario
23 alerts
Closed alerts
within this scenario
Closed as TP
within this scenario
Closed as FP
within this scenario
0 alerts
Welcome to SOC Simulator.
Get hands-on experience with threat actor TTPs in a safe, simulated environment to improve you and your team's security posture.
Powered by Navattic
1 of 11
Next
Alert types
23
Alerts
Sort by
Severity
monitor new alerts as they arrive.
email from external domain. Low Phishing
Low Phishing
1020 Suspicious email from external domain. Low Phishing
1019 Reply to suspicious email. Low Phishing
1018 Suspicious Parent Child Relationship Low Process
1017 Suspicious Attachment found in email Low Phishing
ENG
15:06


tryhackme.com/soc-sim/
Click to go forward, hold to see history
Dive into the heat of a live phishing attack as it unfolds within the corporate network.
Scenario details
Dashboard
Alert queue
SIEM
My computer
Documentation
Playbooks
Case reports
Guide
Exit simulation
Total alerts
within this scenario
23 alerts
Closed alerts
within this scenario
0 alerts
Closed as TP
within this scenario
0 alerts
Closed as FP
within this scenario
0 alerts
Alert types
Alert types
Alert severity
23
Alerts
Execution 0 alerts
Phishing 15 alerts
Process 8 alerts
Open alerts
Sort by
Severity
Access the alert queue to monitor new alerts as they arrive.
Experience realtime attacks.
Alerts trigger in realtime as threat actor events unfold throughout a scenario.
Back
2 of 11
Next
Low Phishing
Low Phishing
Low Phishing
Low Phishing
Low Process
1017 Suspicious Attachment found in email Low Phishing


Dashboard
try hack me free - Google Sear
TryHackMe | TryHack3M: Bricks
tryhackme.com/soc-sim/
Click to go forward, hold to see history
Alert queue
Assigned alert
You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. Learn more
Search for an alert
Reset filters
Severity
Status
Alert type
Show 15 alerts
ID
Alert rule
Severity
Type
Date
Status
Action
1023
Suspicious email from external domain.
Low
Phishing
Dec 16th 2024 at 20:28
Awaiting action
Description:
datasource:
timestamp:
subject:
sender:
recipient:
attachment:
content:
direction:
unusual top level domain. Note from SOC Head: This detection rule still
ow!
privacy regulations and company security policies to protect sensitive
Triage attacks in realistic alert queues.
Take ownership of alerts you need to investigate based on their type, severity, and recency.
Back
3 of 11
Next
1022
Suspicious email from external domain.
4 at 20:27
Awaiting action
1021
Reply to suspicious email.
Low
Phishing
Dec 16th 2024 at 20:27
Awaiting action
1020
Suspicious email from external domain.
Low
Phishing
Dec 16th 2024 at 20:27
Awaiting action
Dashboard
Alert queue
SIEM
My computer
Documentation
Playbooks
Case reports
Guide
Exit simulation


tryhackme.com/soc-sim/
Alert queue
Assigned alert
Dashboard
Alert queue
SIEM
My computer
Documentation
Playbooks
Case reports
Guide
Exit simulation
Perform forensics on malicious artifacts.
Use real-world tooling to investigate suspicious links, files and IPs to uncover the cyber kill chain in a dedicated, browser-based virtual machine.
Back
4 of 11
Next
lert to start investigating and find all the true positives. Learn more
Reset filters
Severity
Status
Alert type
Show 15 alerts
Severity
Type
Date
Status
Action
Low
Phishing
Dec 16th 2024 at 20:28
Awaiting action
A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Head: This detection rule still needs fine-tuning.
emails
16/12/2024 20:28:16.806
Secret Island Getaway: Claim Your FREE Hat-Themed Vacation Now!
sender:
le@modernmillinerygroup.online
recipient:
michelle.smith@tryhatme.com
attachment:
None
content:
The content of this email has been removed in accordance with privacy regulations and company security policies to protect sensitive information.
direction:
inbound
1022
Suspicious email from external domain.
Low
Phishing
Dec 16th 2024 at 20:27
Awaiting action
1021
Reply to suspicious email.
Low
Phishing
Dec 16th 2024 at 20:27
Awaiting action
1020
Suspicious email from external domain.
Low
Phishing
Dec 16th 2024 at 20:27
Awaiting action


Reload this page
ckme.com/soc-sim/
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
1 win-3450
All time
✓ 99 events (before 11/7/24 10:36:37.000 PM)
No Event Sampling
Job
Verbose Mode
Events (99)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 minute per column
List
Format
50 Per Page
< Prev
1
2
Next >
Investigate event logs in Splunk.
Determine true from false positives using a live Splunk instance congested with benign network traffic to simulate realistic SIEM environments.
Back
5 of 11
Next
Event
{ [-]
datasource: sysmon
event.action: Registry value set (rule: RegistryEvent)
event.code: 13
host.name: win-3450
process.pid: 3868
registry.key: System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion
registry.path: HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion
registry.value: DriverVersion
timestamp: 01/08/2024 08:53:49.000
}
Show as raw text
host = eventcollector
source = logs.json
sourcetype = _json
1/8/24
8:43:40.000 AM
{ [-]
datasource: sysmon


tryhackme.com/soc-sim/
00:00:55
Case report for event ID: 1023
ID
Alert rule
Description
Incident type
Severity level
Date and time detected
1023
Suspicious email from external domain.
A suspicious email was received from an extern
sender with an unusual top level domain. Note
SOC Head: This detection rule still needs fine-t
Dec 16th 2024 at 20:28
Alert details
Dashboard
Alert queue
SIEM
My computer
Documentation
Playbooks
Case reports
Guide
Exit simulation
Close out alerts with written reports.
Based on your investigations, document your findings and make suggestions for eradication, containment and recovery to the IR team.
Back
6 of 11
Next
Incident report
Incident classification
True positive
Case report
Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.
The investigation into host win-3450 revealed several related alerts that warranted further scrutiny. Notably, the parent process involved in the suspicious activity was identified as 'powershell.exe', which is atypical for a non-technical user to employ. This anomaly raised significant concerns about potential misuse. Additionally, the activity was linked to the network drive FinancialRecords, a repository likely containing sensitive financial information at risk of exfiltration. Given these findings, the suspicious activity on win-3450 is concerning, indicating a need for immediate isolation of the host, a comprehensive forensic analysis, and enhanced security measures to protect sensitive data.

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1015	Suspicious Attachment found in email	A suspicious attachment was found in the email. Investigate further to determine if it is malicious.	Phishing	Low	Sep 4th 2024 at 14:57

Incident classification — ✓ True positive — + 10 points

Instant feedback, powered by AI.

Get qualitative and quantitative feedback on your incident reports based on correctly documenting and identifying all of the IoCs and techniques the attacker used.

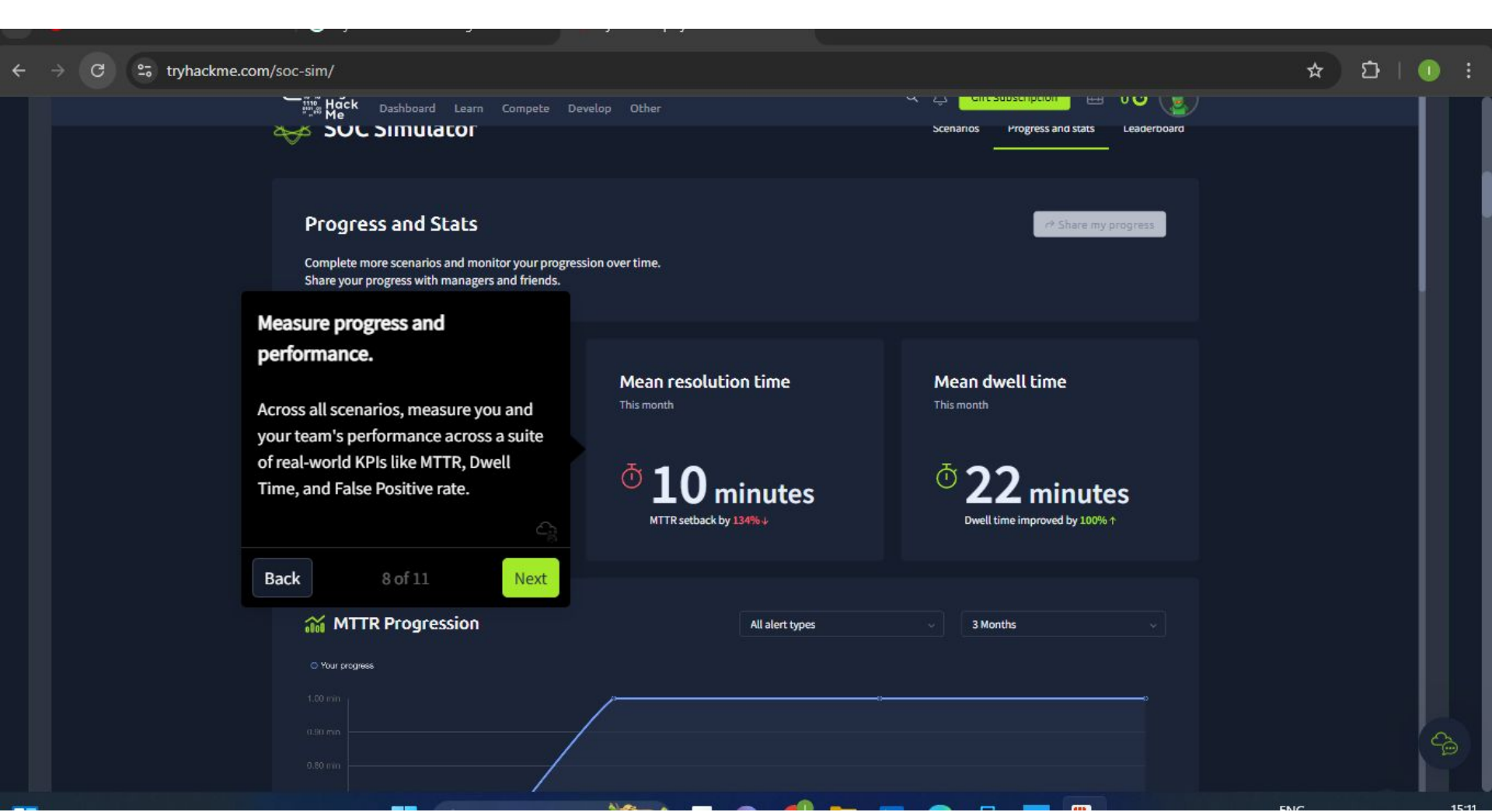
Back — 7 of 11 — Next

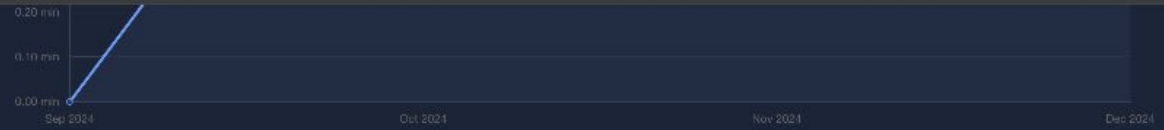
✓ Correct process. + 60 points

The investigation into the suspicious email revealed it originated from an .xyz domain, often associated with malicious activity. The email's subject line employed urgent language, a common characteristic of scams or spam. Upon opening the email, the user, michael.ascot, downloaded an attached zip file. This zip file contained a script disguised with a 'pdf.lnk' extension, which is malicious because it appears to be a harmless PDF but is actually an executable script. The user inadvertently executed the script, which then downloaded the Powercat PowerShell module from GitHub. Powercat was used to establish a reverse tunnel proxy, enabling unauthorized remote access to the user's system.

→ Excellent work on this analysis. You comprehensively covered all aspects of the suspicious email, from its origin to the final impact of the malicious script. Your detailed explanation of the threat vector helps in understanding the potential damage and the method used by attackers. Keep up the thorough and precise evaluations.

Does this alert require escalation? — ✗ Escalation


tryhackme.com/soc-sim/
Hack Me
Dashboard
Learn
Compete
Develop
Other
Gift Subscription
SOC Simulator
Scenarios
Progress and stats
Leaderboard
Progress and Stats
Share my progress
Complete more scenarios and monitor your progression over time.
Share your progress with managers and friends.
Measure progress and performance.
Across all scenarios, measure you and your team's performance across a suite of real-world KPIs like MTTR, Dwell Time, and False Positive rate.
Back
8 of 11
Next
Mean resolution time
This month
10 minutes
MTTR setback by 134% ↓
Mean dwell time
This month
22 minutes
Dwell time improved by 100% ↑
MTTR Progression
All alert types
3 Months
Your progress
1.00 min
0.80 min
0.60 min



True positive identification rate

Rate of incidents co

All alert types

Identify skill gaps.

Drill down into each KPI and specific alert types to easily identify where you and your team should focus your training.

Back 10 of 11 Next

Your true positive rate is excellent! Keep up the great work!

False positive identification rate

Rate of incidents correctly identified as benign

All alert types

Your false positive rate is solid, but there's room for improvement. Keep striving!

True positive rate identification progression

All alert types

3 Months

Your progress